

# EQUIDISTRIBUTION OF HECKE POINTS ON THE SUPERSINGULAR MODULE

RICARDO MENARES

ABSTRACT. For a fixed prime  $p$ , we consider the (finite) set of supersingular elliptic curves over  $\overline{\mathbb{F}}_p$ . Hecke operators act on this set. We compute the asymptotic frequency with which a given supersingular elliptic curve visits another under this action.

## 1. INTRODUCTION

Let  $p$  be a prime number. We denote by  $E = \{E_1, \dots, E_n\}$  the set of isomorphism classes of supersingular elliptic curves over  $\overline{\mathbb{F}}_p$ . We denote by  $S := \bigoplus_{i=1}^n \mathbb{Z}E_i$  the supersingular module in characteristic  $p$  (i.e.  $S$  is the free abelian group spanned by the elements of  $E$ ). Hecke operators act on  $S$  by

$$T_1 := id, \quad T_m(E_i) = \sum_C E_i/C, \quad m \geq 2,$$

where  $C$  runs through the subgroup schemes of  $E_i$  of rank  $m$ . This definition is extended by linearity to  $S$  and to  $S_{\mathbb{R}} := S \otimes \mathbb{R}$ . For an integer  $m \geq 1$  we put

$$B_{i,j}(m) = |\{C \subset E_i, \quad |C| = m \text{ and } E_i/C \cong E_j\}|.$$

We have that  $T_m E_i = \sum_{j=1}^n B_{i,j}(m) E_j$ . The matrix  $(B_{i,j}(m))_{i,j=1}^n$  is known as the Brandt matrix of order  $m$ .

For a given  $D = \sum_{i=1}^n a_i E_i \in S_{\mathbb{R}}$ , we put  $\deg D = \sum_{i=1}^n a_i$ . We have that ([4], Proposition 2.7)

$$\deg T_m E_i = \sum_{\substack{d|m \\ p \nmid d}} d =: \sigma(m)_p,$$

leading to define  $\deg T_m := \sigma(m)_p$ .

Let  $M$  be the set of probability measures on  $E$ . For every  $i = 1, \dots, n$ , we denote by  $\delta_{E_i} \in M$  the Dirac measure supported on  $E_i$ . Let

$$S^+ := \left\{ \sum_{i=1}^n a_i E_i \in S_{\mathbb{R}} \text{ such that } a_i \geq 0 \right\} - \{0\}.$$

For any  $D = \sum_{i=1}^n a_i E_i \in S^+$ , we put

$$\Theta_D := \frac{1}{\deg D} \sum_{i=1}^n a_i \delta_{E_i}.$$

We have that  $\Theta_D$  is a probability measure on  $E$  and every element of  $M$  has this form. Hence, there is a natural action of the Hecke operators on  $M$ , given by  $T_m \Theta_D := \Theta_{T_m D}$ .

Each  $E_i$  has a finite number of automorphisms. We define

$$w_i := |\text{Aut}(E_i)/\{\pm 1\}|, \quad W := \sum_{i=1}^n \frac{1}{w_i}.$$

The element  $e := \sum_{i=1}^n \frac{1}{w_i} E_i \in S \otimes \mathbb{Q}$  is Eisenstein ([4], p. 139), i.e.

$$(1.1) \quad T_m(e) = \deg T_m e.$$

We denote by  $\Theta := \Theta_e$ . Equation (1.1) implies that  $T_m \Theta = \Theta$  for all  $m \geq 1$ .

Let  $C(E) \cong \mathbb{C}^n$  be the space of complex valued functions on  $E$ . For  $f \in C(E)$ , we denote by  $\|f\| = \max_i |f(E_i)|$  and

$$\Theta_D(f) := \int_E f \Theta_D = \frac{1}{\deg D} \sum_{i=1}^n a_i f(E_i).$$

For a positive integer  $m$ , we write  $m = p^k m_p$  with  $p \nmid m_p$ . In this note, we will prove the following result:

**Theorem 1.1.** *For all  $i = 1, \dots, n$ , the sequence of measures  $\{\Theta_{T_m E_i}\}$ , where  $m$  runs through a set of positive integers such that  $m_p$  grows to infinity, is equidistributed with respect to  $\Theta$ . More precisely, for all  $\varepsilon > 0$ , there exists  $C_\varepsilon > 0$  such that, for every  $f \in C(E)$ , and for every sequence of integers  $m$  such that  $m_p \rightarrow \infty$ , we have that*

$$|\Theta_{T_m E_i}(f) - \Theta(f)| \leq C_\varepsilon \|f\| n m^{-\frac{1}{2} + \varepsilon}.$$

We study the asymptotic frequency of the multiplicity of  $E_j$  inside  $T_m E_i$ . That is, we investigate the behaviour of the ratio  $B_{i,j}(m)/\deg(T_m)$  when  $m$  varies. We will prove Theorem 1.1 in the equivalent formulation:

**Theorem 1.2.** *For all  $\varepsilon > 0$ , there exists  $C_\varepsilon > 0$  such that for every sequence of integers  $m$  such that  $m_p \rightarrow \infty$ , we have that*

$$(1.2) \quad \left| \frac{B_{i,j}(m)}{\deg T_m} - \frac{12}{w_j(p-1)} \right| \leq C_\varepsilon m^{-\frac{1}{2} + \varepsilon}.$$

In particular,

$$(1.3) \quad \lim_{m_p \rightarrow \infty} \frac{B_{i,j}(m)}{\deg T_m} = \frac{12}{w_j(p-1)}.$$

The proof of this assertion is found in section 1.2.

**Remark 1.3.** The equality  $\sum_{j=1}^n \frac{B_{i,j}(m)}{\deg T_m} = 1$ , combined with equation (1.3) implies the mass formula of Deuring and Eichler:

$$W = \sum_{j=1}^n \frac{1}{w_j} = \frac{p-1}{12}.$$

Theorem 1.1 can be deduced from Theorem 1.2 as follows: remark 1.3 implies that  $\Theta = \sum_{j=1}^n \frac{12}{w_j(p-1)} \delta_{E_j}$ . Take  $f \in C^0(E)$ . We have that

$$|\Theta_{T_m E_i}(f) - \Theta(f)| \leq \|f\| \sum_{j=1}^n \left| \frac{B_{i,j}(m)}{\deg T_m} - \frac{12}{w_j(p-1)} \right|.$$

Hence, inequality (1.2) implies Theorem 1.1.

Let  $h : E \rightarrow E$  be a function. Then  $h$  defines an endomorphism of  $S$  and of  $S_{\mathbb{R}}$  by the rule

$$h\left(\sum a_i E_i\right) := \sum a_i h(E_i).$$

We will also consider the action induced on  $M$  by  $h^* \Theta_D := \Theta_{h(D)}$ .

**Corollary 1.4.** *Let  $q \neq p$  be a prime number. Let  $h : E \rightarrow E$  be a function such that  $h \circ T_q = T_q \circ h$ . Then  $h^* \Theta = \Theta$ . In other words,  $h$  can be identified with a permutation  $\tau \in S_n$  by  $h(E_i) = E_{\tau(i)}$  and we have that  $w_i = w_{\tau(i)}$  for all  $i = 1, \dots, n$ .*

**Proof:** since  $T_{q^k}$  is a polynomial in  $T_q$ , we also have that  $h \circ T_{q^k} = T_{q^k} \circ h$ . Let  $f \in C(E)$ . We have that

$$\begin{aligned}
 (1.4) \quad h^* \Theta(f) &= \lim_{k \rightarrow \infty} h^* \Theta_{T_{q^k} E_1}(f) \\
 &= \lim_{k \rightarrow \infty} \Theta_{h \circ T_{q^k} E_1}(f) \\
 &= \lim_{k \rightarrow \infty} \Theta_{T_{q^k}(h(E_1))}(f) \\
 (1.5) \quad &= \Theta(f),
 \end{aligned}$$

where we have used Theorem 1.1 in (1.4) and (1.5) ■

The statement Theorem 1.1, using the Hecke invariant measure  $\Theta$ , has been included to emphasize the analogy with the fact that Hecke orbits are equidistributed on the modular curve  $SL_2(\mathbb{Z}) \backslash \mathbb{H}$  with respect to the hyperbolic measure, which is Hecke invariant (e.g. see [1], Section 2).

**1.1. Weight 2 Eisenstein series for  $\Gamma_0(p)$ .** The modular curve  $X_0(p)$  has two cusps, represented by 0 and  $\infty$ . We denote by  $\Gamma_\infty$  (resp.  $\Gamma_0$ ) the stabilizer of  $\infty$  (resp. 0). The associated weight 2 Eisenstein series are given by

$$\begin{aligned}
 E_\infty(z) &= \frac{1}{2} \lim_{\varepsilon \rightarrow 0^+} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(p)} j_\gamma(z)^{-2} |j_\gamma(z)|^{-2\varepsilon} \\
 E_0(z) &= \frac{1}{2} \lim_{\varepsilon \rightarrow 0^+} \sum_{\gamma \in \Gamma_0 \backslash \Gamma_0(p)} j_{\sigma_0^{-1}\gamma}(z)^{-2} |j_{\sigma_0^{-1}\gamma}(z)|^{-2\varepsilon},
 \end{aligned}$$

where  $\sigma_0 = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & 0 \end{pmatrix}$  and  $j_\eta(z) = cz + d$  for  $\eta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ .

The functions  $E_\infty$  and  $E_0$  are weight 2 modular forms for  $\Gamma_0(p)$  and they are Hecke eigenforms. The Fourier expansions at  $i\infty$  are ([5], Theorem 7.2.12, p. 288)

$$\begin{aligned}
 E_\infty(z) &= 1 - \frac{3}{\pi y(p+1)} + \frac{24}{p^2-1} \sum_{n=1}^{\infty} b_n q^n \\
 E_0(z) &= -\frac{3}{\pi y(p+1)} - \frac{24p}{p^2-1} \sum_{n=1}^{\infty} a_n q^n,
 \end{aligned}$$

with the sequences  $a_n$  and  $b_n$  given by:

- if  $p \nmid n$ , then  $a_n = b_n = \sigma_1(n) = \sum_{d|n} d$
- if  $k \geq 1$ , then  $b_{p^k} = p + 1 - p^{k+1}$  and  $a_{p^k} = p^k$
- if  $p \nmid m$  and  $k \geq 1$ , then  $b_{p^k m} = -b_{p^k} b_m$  and  $a_{p^k m} = a_{p^k} a_m$ .

By taking an appropriate linear combination, we obtain a non cuspidal, holomorphic at  $i\infty$  modular form

$$\begin{aligned}
f_0(z) &:= E_\infty(z) - E_0(z) \\
&= 1 + \frac{24}{p^2 - 1} \sum_{n=1}^{\infty} (pa_n + b_n)q^n.
\end{aligned}$$

Since we have that

$$\begin{aligned}
E_\infty|_{\sigma_0}(z) &= E_0(z) \\
E_0|_{\sigma_0}(z) &= E_\infty(z),
\end{aligned}$$

this shows that  $f$  is holomorphic at  $\Gamma_0(p)0$  as well. Since

$$\dim_{\mathbb{C}} M_2(\Gamma_0(p)) = 1 + \dim_{\mathbb{C}} S_2(\Gamma_0(p))$$

and since  $f$  is holomorphic, non zero and non cuspidal, we have the decomposition

$$(1.6) \quad M_2(\Gamma_0(p)) = S_2(\Gamma_0(p)) \oplus \mathbb{C}f_0.$$

**1.2. Proof of Theorem 1.2.** Recall that we write  $m = p^k m_p$  with  $p \nmid m_p$ . We have that  $B(p^k)$  is a permutation matrix of order dividing 2 and that  $B(m) = B(p^k)B(m_p)$  ([4], Proposition 2.7). It follows that  $\deg(T_m) = \deg(T_{m_p})$  and that we can define, for each  $i = 1, \dots, n$ , an index  $i(k) \in \{1, \dots, n\}$  such that  $B_{i,l}(p^k) = \delta_{i(k),l}$ . Furthermore,  $i(k) = i$  if  $k$  is even. We have that

$$\begin{aligned}
\frac{B_{i,j}(m)}{\deg T_m} &= \sum_{l=1}^n \frac{B_{i,l}(p^k)B_{l,j}(m_p)}{\deg T_{m_p}} \\
&= \frac{B_{i(k),j}(m_p)}{\deg T_{m_p}}.
\end{aligned}$$

Hence, to prove Theorem 1.2 we may assume  $p \nmid m$ , which is what we will do in what follows.

Our method is based on the interpretation of the multiplicities  $B_{i,j}(m)$  as Fourier coefficients of a modular form.

**Theorem 1.5.** *For every  $0 \leq i, j \leq n$ , there exists a weight 2 modular form  $f_{i,j}$  for  $\Gamma_0(p)$  such that its  $q$ -expansion at  $\infty$  is*

$$f_{i,j}(z) := \frac{1}{2w_j} + \sum_{m=1}^{\infty} B_{i,j}(m)q^m, \quad q = e^{2\pi iz}.$$

**Proof:** this fact is stated in [4], p.118. It is a particular case of [3], Chapter II, Theorem 1 ( $D = p, H = 1, l = 0$  in Eichler's notation). We remark that the theorem in *loc. cit.* states modularity of a theta series constructed from an order in a quaternion algebra. The fact that this theta series is the same as our  $f_{i,j}$  is a consequence of [4], Proposition 2.3 ■

Using (1.6), we can decompose

$$f_{i,j} = g_{i,j} + c_{i,j}f_0, \quad g_{i,j} \in S_2(\Gamma_0(p)), \quad c_{i,j} \in \mathbb{C}.$$

Comparing the  $q$ -expansions, we get  $c_{i,j} = \frac{1}{2w_j}$ . We have that

$$g_{i,j} = f_{i,j} - c_{i,j}f_0 = \sum_{m=1}^{\infty} c_m q^m,$$

where

$$c_m = B_{i,j}(m) - \frac{12}{w_j(p^2 - 1)}(pa_m + b_m).$$

The coefficient  $c_m$  depends on  $(i, j)$ , but we don't include this dependence in the notation in order to simplify it. Since  $p \nmid m$ , we have that  $\deg(T_m) = \sigma_1(m)$  and

$$c_m = B_{i,j}(m) - \frac{12}{w_j(p - 1)}\sigma_1(m).$$

Hence,

$$\begin{aligned} \left| \frac{B_{i,j}(m)}{\deg T_m} - \frac{12}{w_j(p - 1)} \right| &= \frac{|c_m|}{\sigma_1(m)} \\ &\leq \frac{|c_m|}{m}. \end{aligned}$$

Using Deligne's theorem ([2], théorème 8.2, previously Ramanujan's conjecture), we have that

$$c_m = O_{\varepsilon}(m^{1/2+\varepsilon}),$$

concluding the proof. ■

## REFERENCES

- [1] Laurent Clozel and Emmanuel Ullmo. Équidistribution des points de Hecke. In *Contributions to automorphic forms, geometry, and number theory*, pages 193–254. Johns Hopkins Univ. Press, Baltimore, MD, 2004.
- [2] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.
- [3] M. Eichler. The basis problem for modular forms and the traces of the Hecke operators. In *Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 75–151. Lecture Notes in Math., Vol. 320. Springer, Berlin, 1973.
- [4] Benedict H. Gross. Heights and the special values of  $L$ -series. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 115–187. Amer. Math. Soc., Providence, RI, 1987.
- [5] Toshitsune Miyake. *Modular forms*. Springer-Verlag, Berlin, 1989. Translated from the Japanese by Yoshitaka Maeda.